RAPPORT 13 DECEMBER 2006

DNR 06-11714-601

2006:18

Operativa risker

- företagens hantering och FI:s rekommendationer

INNEHÅLL

FÖRORD 3

SAMMANFATTNING 4

INTRODUKTION 5
- Operativa risker 5
- Schablonmetoden för kapitaltäckning av operativa risker 5
- Finansinspektionens granskningsarbete 6
- Komponenter i ett riskhanteringssystem 7

IDENTIFIERING OCH VÄRDERING AV OPERATIVA RISKER 8
- Generellt om analys av operativa risker 8
- Självutvärdering av operativa risker 8
- Processbaserad riskanalys 9
- Incident- och förlustdatabaser 9
- Analys av risker i nya produkter 10
- Riskindikatorer 10
- Finansinspektionens rekommendationer 10

STYRNING AV OPERATIVA RISKER 12
- Styrdokument för operativa risker 12
- Toleransnivåer för operativa risker 12
- Styrning av riskprofilen 12
- Kontinuitetsplanering 13
- Finansinspektionens rekommendationer 13

ORGANISATION OCH RAPPORTERING 15
- Organisation och ansvarsfördelning 15
- Riskrapportering 15
- Finansinspektionens rekommendationer 16

FORTSATT UTVECKLING 17

Förord

Finansinspektionen har under hösten 2005 och våren 2006 genomfört en omfattande granskning av hanteringen av operativa risker i femton svenska banker och kreditmarknadsföretag. Granskningen har gjorts på företagens begäran som en del av prövningen av hur de efterlever bestämmelserna i regelverket om schablonmetoden för kapitaltäckning av operativa risker. FI har granskat företagens styr- och metoddokument och gjort platsbesök för att undersöka hur metoderna är införda i organisationerna.

I rapporten sammanfattas nuläget för hanteringen av operativa risker i de berörda företagen. Syftet är att ge en bild av vad som är praxis för riskanalysmetoder, riskstyrningsmekanismer och riskorganisation. Rapporten berör inte avancerade interna metoder för att kvantifiera operativa risker.

FI:s syn på de olika frågorna presenteras för vart och ett av de områden som berörs. Det ska dock betonas att detta endast är rekommendationer som till viss del går utöver de krav som ställs i regelverket för schablonmetoden. Det kan finnas andra lösningar än de föreslagna som är helt förenliga med reglerna.

Sammanfattning

På begäran har Finansinspektionen under hösten 2005 och våren 2006 granskat hanteringen av operativa risker i femton företag och granskningen har gett FI en god överblick över marknaden.

Företagen identifierar och värderar operativa risker med någon form av självutvärderingsmetod där riskerna bedöms utifrån sannolikhet och konsekvens. Självutvärderingen kompletteras i vissa fall med riskindikatorer. De företag som FI har granskat har också infört eller håller på att införa en strukturerad lagring av förlust- och incidentdata.

På övergripande nivå råder konsensus på marknaden om vilka metoder som ska användas för att hantera operativa risker, men det finns stora skillnader i hur metoderna har implementerats och hur långt företagen har kommit med att tillämpa dem.

De flesta av företagen styr sina operativa risker genom bland annat åtgärdsplaner som är kopplade till självutvärderingsverktyget. Därtill påverkas förstås den operativa riskprofilen av många andra beslut som tas i organisationen inklusive styrelsen. Ett annat verktyg för styrning av operativa risker är kontinuitetsplaneringen. Denna är utformad på olika sätt i olika företag men innefattar i samtliga fall någon form av krisorganisation, reservlösningar för el, telefoni, IT-system och liknande.

Den funktion som ansvarar för kontroll av operativa risker är för det mesta underställd en befattningshavare som i sin tur rapporterar till företagets vd. En rapportering som innehåller en koncernövergripande risksammanställning som lämnas till styrelsen, normalt halvårsvis. Rapporteringen innehåller alla operativa risker, inklusive dem som är kopplade till regelefterlevnad och säkerhetsfrågor. Säkerhetsorganisationen är i vissa fall en del av organisationen för operativa risker. I andra fall får riskkontrollenheten rapportering från säkerhetsorganisationen för att styrelserapporteringen om operativa risker ska bli komplett.

FI rekommenderar att företagens styrelser har en aktiv roll i riskhanteringen och sätter dess yttersta ramar i alla väsentliga avseenden. Ett antal verktyg bör användas för att identifiera och värdera operativa risker: självutvärdering eller processbaserad riskanalys, riskindikatorer och analys av incident- och förlustdata. Riskanalysen bör täcka alla operativa risker och rapporteras till styrelsen. Ansvaret för central analys och kontroll av operativa risker bör ligga hos en riskkontrollenhet som är direkt underställd vd.

Introduktion

Operativa risker

Operativ risk definieras som risken för förluster till följd av icke ändamålsenliga eller misslyckade interna processer, mänskliga fel, felaktiga system eller externa händelser. Typiska exempel på operativa risker kan vara risken för handhavandefel vid manuella moment i processer, nyckelpersonberoende, risken för bedrägerier eller brott mot interna instruktioner, systemtillgänglighetsrisker och risken för rån.

Operativa risker skiljer sig från kreditrisker och marknadsrisker genom att ett kreditinstitut ytterst sällan medvetet tar på sig operativa risker för att tjäna pengar. Undantag från detta är exempelvis tjänster som innebär att företaget tar över viss verksamhet från sina kunder (*insourcing*).

Schablonmetoden för kapitaltäckning av operativa risker

Inom EU implementeras just nu det nya kapitaltäckningsregelverk för kreditinstitut som baseras på Basel 2-överenskommelsen. Regelverket innehåller bestämmelser för hur kapitalkravet ska beräknas för kreditrisker, marknadsrisker, operativa risker och övriga risker.

För operativa risker ger det nya kapitaltäckningsramverket tre möjliga metoder:

- *basmetoden*, där kapitalkravet bestäms som en intäktsindikator multiplicerat med 15 procent
- *schablonmetoden*, som fungerar på samma sätt men med olika procentsatser för olika affärsområden
- *internmätningsmetoder*, där företaget självt bygger statistiska modeller för att kvantifiera sina operativa risker baserat på historiska data.

I regelverket för schablonmetoden finns ett antal kvalificeringskriterier som företagen måste uppfylla för att få använda metoden. Det handlar om krav på:

- styrdokument för operativa risker
- riskhanteringsprocesser
- dokumenterad riskhantering
- styrning och kontroll
- rapportering
- beräkning av intäktsindikatorn.

Finansinspektionens föreskrift FFFS 2005:19 om att mäta och hantera operativ risk, i vilka schablonmetoden regleras, finns på www.fi.se.

Finansinspektionens granskning

FI har under hösten 2005 och våren 2006 granskat hanteringen av operativa risker i de företag som har begärt en sådan granskning i enligt lagen om kapitaltäckning och stora exponeringar för kreditinstitut och värdepappersbolag.[1] Femton företag, både stora och små banker, sparbanker och kreditmarknadsföretag begärde att få sin metod för hantering av operativa risker granskad.

Granskningsarbetet genomfördes i två steg:

- analys av företagens riskhantering med utgångspunkt i den dokumentation som de har skickat till FI
- platsundersökningar – granskning av riskhanteringen i praktiken, hur riskhanteringsprocesserna är implementerade och huruvida företagen följer fastställda instruktioner.

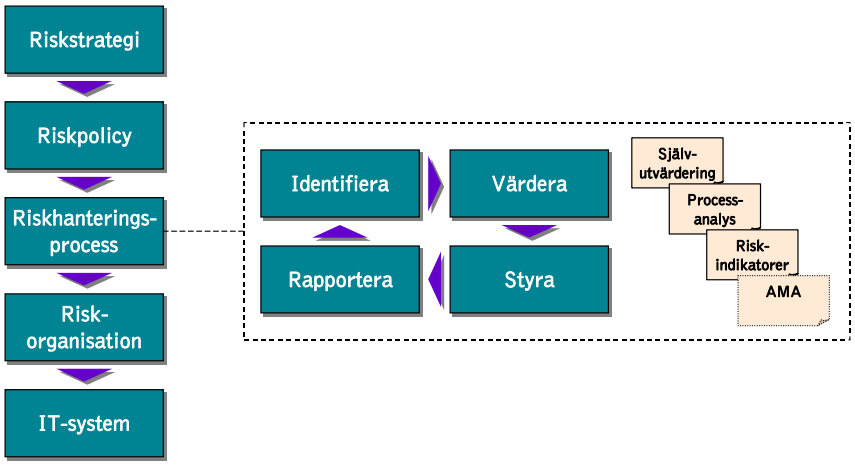
Inom ramen för platsundersökningarna besökte FI både den centrala riskkontrollorganisationen, olika lokala eller regionala organisationer och, i förekommande fall, investmentbankverksamheten och utländsk filial eller utländskt dotterbolag.

Under granskningens gång har FI påtalat identifierade brister i hanteringen till samtliga företag. Efter skrivbordsundersökningen hade alla företagen underkänts beträffande kraven på styrdokument och flera hade brister i sin rapportering. Dessa brister har därefter i de flesta fallen åtgärdats. Efter avslutad granskning uppfyller merparten av företagen större delen av regelverkets krav.

Granskningsarbetet har gett FI en mycket god överblick över marknadens hantering av operativa risker. Vid en jämförelse med motsvarande situation för ett par år sedan är det tydligt att det nya regelverket har bidragit till att driva på utvecklingen mot förbättrad riskhantering. FI har också uppfattat att man i många företag börjar se en konkret affärsnytta i att ha en strukturerad process för att identifiera operativa risker.

[1] 7 kap.13 d § 2 i lagen (1994:2004) om kapitaltäckning och stora exponeringar för kreditinstitut och värdepappersbolag

Komponenter i ett riskhanteringssystem



Det är viktigt att riskhanteringen i ett kreditinstitut är genomtänkt på strategisk nivå. Riskprofilen bör i möjligaste mån vara ett resultat av medvetna beslut, även ifråga om operativa risker. Operativa risker bör vara en komponent vid större beslut som påverkar den operativa verksamheten.

Riskstrategin formaliseras genom en riskpolicy och andra styrdokument, som också normalt innehåller krav på riskhanteringsprocessen, metoder och verktyg som används, riskorganisationen och riskrapporteringen.

Riskhanteringsprocessen omfattar på den mest övergripande nivån identifiering och värdering av risker, åtgärder för att styra riskprofilen samt rapportering av riskerna. Processen stöds av olika analysverktyg som självutvärderingar, processbaserad riskanalys, riskindikatorer eller avancerade interna modeller.

Riskorganisationen omfattar alla befattningshavare som har en roll i riskhanteringsprocessen, inklusive riskkontrollenhet, styrelse, vd, ansvariga för operativa risker inom olika delar av företaget, linjechefer med flera.

Behovet av IT-systemstöd är ofta mer begränsat för operativa risker än för marknads- eller kreditrisker. Det som normalt används är en incidentdatabas med ett lämpligt gränssnitt för rapportering och, i vissa fall, systemstöd för självutvärderingsmetoder.

De följande kapitlen i denna rapport har strukturerats med utgångspunkt i den generiska riskhanteringsprocessen enligt ovan. Först beskrivs de verktyg för identifiering och värdering av risker som används, därefter mekanismer för riskstyrning och, slutligen, rapporteringen. I samband med rapporteringen behandlas också riskorganisationsfrågor.

Identifiering och värdering av operativa risker

Generellt om analys av operativa risker

Medan marknads- och kreditriskområdena numera har fått en arsenal av avancerade modeller för kvantifiering av risker befinner sig operativriskområdet fortfarande i ett läge där kvalitativa, subjektiva analysmetoder är vanligast. Två huvudtyper av analysmetoder kan identifieras: självutvärdering och processbaserad riskanalys.

Riskerna bedöms i regel i termer av sannolikhet respektive konsekvens på skalor i fyra eller fem steg. I de flesta av fallen kopplas konsekvensdimensionen till monetära värden. Ofta varierar emellertid värderingsgrunderna inom en stor organisation för att var och en av de organisatoriska enheterna ska ha nytta av riskvärderingen för sin egen del; det som är en väsentlig risk för ett litet affärsområde kanske är helt obetydlig för ett stort. Detta innebär att det är en utmaning att samla ihop riskerna på koncernnivå. Riskkontrollenheten har därför ofta en viktig roll i analysen genom att göra en övergripande samlad bedömning i dialog med de olika delarna av organisationen.

Att utforma och införa en analysmetod av detta slag tar i regel ganska lång tid. Det dröjer ofta ett antal år innan organisationen har lärt sig att använda metoden och använder den på ett likformigt sätt.

Som komplement till subjektiva metoder mäts ofta riskindikatorer (se nedan).

Självutvärdering av operativa risker

Den absolut vanligaste typen av analysmetod för operativa risker är självutvärderingen. Det exakta tillvägagångssätt som används för att bedöma operativa risker genom självutvärdering varierar emellertid i stor omfattning mellan företagen.

En självutvärdering genomförs normalt en gång om året i en workshop med befattningshavare som har kunskap om olika delar av den process eller organisation som ska analyseras. Riskidentifieringen stöds i vissa fall av formulär med fördefinierade riskområden där deltagarna kan fylla i värderingen av riskernas sannolikhet och konsekvens. I praktiken är det i detta avseende stor skillnad mellan de företag som har granskats. I vissa fall används formulär där i princip alla risker är fördefinierade och utvärderingen enbart handlar om att värdera riskerna ifråga. I andra fall genomförs självutvärderingen helt utan stöd av fördefinierade risker eller riskkategorier.

Självutvärderingar kan göras för organisatoriska enheter, processer eller IT-system. Vanligast är att analyserna görs per organisatorisk enhet, dock med viss kompletterande analys i processdimensionen.

Även beträffande den organisatoriska nivån på vilken riskanalyserna genomförs finns stora skillnader mellan företagen. I vissa fall görs analysen på en hel region inom Sverige, och i andra fall på lägre nivå. Detta varierar ofta även inom företagen, beroende på riskprofilen och komplexiteten i verksam-

heten i de olika delarna av organisationen. I de fall analysen görs på låg nivå i organisationen kan det vara svårt att täcka hela verksamheten varje år.

Vissa banker har infört system som används för självutvärdering samt för lagring och analys av självutvärderingsdata.

Processbaserad riskanalys

Ett mer strukturerat men något mer tidskrävande alternativ till självutvärderingen är den processbaserade riskanalysen. Metoden går ut på att systematiskt gå igenom processdokumentation, normalt i form av processkartor, och identifiera risker med stöd av en detaljerad riskklassificering. Denna typ av analys kan exempelvis genomföras av en oberoende analytiker i samarbete med processägare och, i de fall det behövs, experter inom de områden som berörs.

Utdata från en processbaserad riskanalys ser typiskt ut på samma sätt som resultatet från en självutvärdering: bedömning av sannolikhet och konsekvens på en skala som normalt har fyra eller fem steg.

Processanalys är mer resursmässigt krävande än självutvärdering, eftersom en komplett processdokumentation måste finnas till hands för analysen och uppdateras kontinuerligt. Att dokumentera viktiga processer är å andra sidan något som har ett stort värde i och för sig eftersom det direkt reducerar den potentiella inverkan av vissa operativa risker, främst nyckelpersonberoenden och andra personalrelaterade risker. Processanalys kan också ge en mer systematisk riskidentifieringsprocess än självutvärdering.

Processbaserad riskanalys är ett betydligt mindre vanligt verktyg än självutvärdering. Verktyget kan vara svårt att använda i en stor, komplex organisation och används inte av någon av de stora banker som har granskats.

Incident- och förlustdatabaser

Samtliga företag som har granskats har någon form av incident- och förlustrapportering, även om den i vissa företag fortfarande befinner sig i ett relativt tidigt utvecklingsskede. Rapporteringen omfattar normalt alla förluster över en viss kvantitativ gräns, ofta 50 000 SEK, och incidenter som var tillräckligt allvarliga men som inte ledde till någon förlust. Tröskelvärdet för rapportering bestäms med utgångspunkt i verksamhetens karaktär och företagets storlek. Normalt rapporteras för varje förlusttillfälle en beskrivning av händelsen, beskrivning av skadan, förlustbeloppet och de åtgärder som vidtagits eller ska vidtas. Incidenterna eller förlusterna kategoriseras ofta med utgångspunkt i de typer av händelser som finns i det nya kapitaltäckningsdirektivet. Informationen lagras i en databas och statistik rapporteras i flera företag till styrelsen periodvis.

En stor utmaning vid införandet av en incident- och förlustdatabas är att åstadkomma en rapportering som täcker alla de incidenter som inträffar. Det är svårt att ge incitament till organisationen att rapportera sådant som har gått fel eller som har varit på väg att gå fel.

Analys av risker i nya produkter

Alla de företag som har granskats har någon form av dokumenterad process för att bedöma risker i nya produkter. Särskilt utvecklat är detta ofta inom investmentbankverksamheten. Processens omfattning är beroende av vilken produkttyp det handlar om. Normalt inkluderar processen följande komponenter:

- kontroll av att produkten kan hanteras i alla berörda delar av organisationen (front-, middle- och back office etc.)
- dokumentation av process eller rutinbeskrivning för den nya produkten
- kontroll av att värderings- och riskmätningsmodeller finns för produkten
- beslut med godkännande av alla berörda linjechefer

Riskindikatorer

Riskindikatorer har typiskt formen av nyckeltal som mäter funktionen hos någon av processerna i verksamheten och vars utveckling följs över tiden. Det kan exempelvis röra sig om att mäta andelen av det totala antalet transaktioner som makuleras, genomsnittlig anställningstid inom en enhet eller antalet limitöverträdelser per period. Syftet är som regel att komplettera de subjektiva riskanalysmetoderna med en mer objektiv uppföljning av observerbara, mätbara storheter som förväntas vara korrelerade med vissa operativa risker.

Det är generellt fortfarande få företag som använder riskindikatorer, men vissa större banker har en välutvecklad användning av verktyget inom investmentbankverksamheten. Vissa företag försöker använda riskindikatorer inom andra delar av verksamheten, men denna utveckling förefaller gå trögt då det är svårt att identifiera lämpliga indikatorer. Skillnaden kan vara motiverad med tanke på att de operativa riskerna generellt är betydligt högre i investmentbankverksamhet än i annan verksamhet.

Finansinspektionens rekommendationer

Alla företag, oavsett storlek, bör ha en väldokumenterad riskanalysmetod utformad efter den verksamhet som bedrivs. Analysen bör vara processorienterad för att på ett korrekt sätt fånga risker som berör flera delar av organisationen.

Det är viktigt att på ett systematiskt sätt identifiera de processer och IT-system som är affärskritiska och säkerställa att dessa analyseras grundligt för operativa risker. Det är också av stor vikt att extrema händelser ägnas tillräcklig uppmärksamhet i riskanalysen, eftersom dessa risker sannolikt inte fångas i interna förlustdatabaser i någon större utsträckning.

Företagen bör också spåra, lagra, analysera och rapportera incident- och förlustdata på ett strukturerat sätt. Dessa data är värdefulla som stöd för riskidentifieringsprocessen men har också ett värde genom att de kan stödja arbetet med effektivisering och förbättring av processer. Den konkreta information om realiserade operativa risker som en fungerande förlustdatabas ger, kan också bidra till att öka medvetenheten om operativa risker i organisationen.

Riskindikatorer bör användas åtminstone inom investmentbankverksamheten men helst inom andra områden också, beroende på riskprofil. Vilka indikatorer som används bör vara beroende av verksamhetens art och av eventuella svagheter hos de processer som analyseras.

För att komplettera analysen av processer och system bör en process också finnas för att analysera risken i nya produkter. Detta gör organisationen medveten om vilken förändring av riskprofilen som en ny produkt medför. Analys av operativa risker bör vara en integrerad del i processen för att utveckla och godkänna nya produkter. Beslutsunderlaget för en ny produkt bör godkännas av alla de delar av organisationen som ska hantera produkten.

Styrning av operativa risker

Styrdokument för operativa risker

Det nya kapitaltäckningsregelverket medför högre krav än tidigare på styrelsernas roll inom de finansiella företagens riskhantering. Detta återspeglas i många fall i de styrdokument för operativa risker som styrelsen fastställer. Bland de företag som har granskats har kvaliteten på styrdokumenten varit varierande. De flesta företagen har under granskningens gång fått mer eller mindre kritik i detta avseende. I vissa fall har ansvaret för att fastställa ramarna för hanteringen av operativa risker delegerats nästan helt till verkställande direktören. I andra fall har styrelsen varit direkt involverad i att ställa krav på alla relevanta aspekter av riskhanteringen.

De företag som är ledande i detta avseende låter styrelsen fastställa

- företagets definition av operativa risker och en kategorisering av riskerna
- konkreta toleransnivåer för operativa risker
- roller och ansvar för styrelse, riskkontrollenhet, affärsområdeschefer, processägare och andra befattningshavare som är inblandade i hanteringen av operativa risker
- vilka verktyg som ska användas för identifiering och värdering av operativa risker, på övergripande nivå
- rapporteringsplan inklusive krav på innehåll i rapporterna
- övergripande principer för utläggning av verksamhet.

Toleransnivåer för operativa risker

Att definiera toleransnivåer för operativa risker är svårt och någon enhetlig praxis har ännu inte utvecklats på marknaden. Företagen har valt olika lösningar för att i styrdokumenten uttrycka hur stora operativa risker som är acceptabla. Vissa företag nöjer sig med att definiera vilka förlustnivåer som inte är acceptabla. Denna lösning ger enbart ett mått på vilket utfall som tolereras snarare än på vilken risk man är beredd att ta i ett framåtblickande perspektiv. Andra företag tar sin utgångspunkt i den riskanalysmetodik som används och relaterar toleransnivån till denna. Exempelvis genom att kräva att åtgärder vidtas när sammanvägningen av sannolikhets- och konsekvensdimensionerna överstiger en viss nivå eller genom att koppla olika risknivåer till olika krav på åtgärder.

Styrning av riskprofilen

Samtliga företag som har granskats använder åtgärdsplaner för hantering av operativa risker som är direkt kopplade till den riskanalysmetod som används. För varje identifierad risk som på grundval av några valda kriterier anses vara väsentlig, fastställs åtgärder som ska vidtas för att minska risken. Åtgärdsplanerna dokumenteras i regel i samband med att riskanalys genomförs.

Det är viktigt att komma ihåg att den operativa riskprofilen är beroende av ett stort antal beslut som fattas inom olika områden; de beslut som blir en

direkt konsekvens av riskanalysen är bara en liten delmängd av dessa. Beslut om exempelvis utläggning av verksamhet, val av IT-plattformar, lansering av nya produkter och liknande kan ha mycket stor påverkan på den totala risknivån.

Kontinuitetsplanering

En viktig komponent i verksamhetens styrning av operativa risker är en väl genomarbetad och anpassad kontinuitetsplan. Den kräver en god analys och beslut om vilka som är de mest skyddsvärda delarna av verksamheten. Kontinuitetsplanering spänner över såväl hot- och sårbarhetsanalys, krisorganisation, inrättande av backup-lösningar samt aktiviteter för att se över fysisk säkerhet, tillgång på extra elförsörjning, telefoni och dylikt. Kontinuitetsplaneringen avser såväl den centrala verksamheten som mer lokal verksamhet på exempelvis ett kontor.

I de granskade företagen finns en skillnad i hur mycket kontinuitetsplaneringen utvecklats. Några organisationer fokuserar på krisorganisationens förmåga att hantera uppkomna situationer där såväl mediekontakter som beslutsfattande planeras och tränas. Andra organisationer utvecklar planerna till att täcka så mycket som möjligt. En gemensam utveckling är att verksamhetens ansvar för planerna är mycket tydlig, processägare och systemägare har ett uttalat ansvar för driften även i ett krisläge. Således finns mycket av kontinuitetsplaneringen genomförd i linjeverksamheten.

IT, telefoni och elförsörjning är av central betydelse för fortsatt verksamhet och här finns ofta väl utvecklade reservlösningar.

Finansinspektionens rekommendationer

Det är av stor vikt att styrelse och ledning är aktivt involverade i företagets riskhantering. Styrelsen bör fastställa de mest övergripande principerna för riskhanteringen:

- riskkategorisering med definitioner
- riskorganisation inklusive ansvarsfördelning mellan styrelsen, riskkontrollenheten och berörda befattningshavare i linjeorganisationen
- metoder och verktyg som ska användas
- rapporteringens innehåll och frekvens
- toleransnivå för operativa risker
- principer för utläggning av verksamhet
- krav på kontinuitetshantering och krisberedskap.

En fastställd riskkategorisering syftar till att skapa en gemensam begreppsapparat för hela organisationen och möjliggöra effektiv rapportering och styrning.

Den toleransnivå för operativa risker som styrelsen fastställer bör på ett eller annat sätt vara kopplad till de bedömningsgrunder eller skalor för värdering av risker som används i företagets riskanalysmetod. Om någon form av modell för allokering av ekonomiskt kapital används, kan denna också vara en naturlig utgångspunkt för att definiera toleransnivån.

De riskanalyser som görs bör vara direkt kopplade till en åtgärdsplan för att reducera de risker som har identifierats och bedömts vara för höga. Åtgärdsplanen bör förutom själva åtgärderna innehålla uppgifter om ansvariga och slutdatum för åtgärderna. Riskanalyserna bör också stödja kontinuerlig förbättring av processer och rutiner.

Beslutsunderlaget för alla större beslut som påverkar den operativa verksamheten (exempelvis utläggning av verksamhet eller etablering av verksamhet i nya länder) bör innehålla en väl genomarbetad analys av hur den operativa riskprofilen påverkas.

Kontinuitetsplaneringen är ett viktigt redskap för att styra de risker som har potentiellt stora negativa konsekvenser. Det är viktigt att organisationen övar de aktiviteter som planlagts och att krisorganisationen fortlöpande tränas.

Organisation och rapportering

Organisation och ansvarsfördelning

Den centrala komponenten i riskorganisationen är riskkontrollenheten. Ofta är det samma organisatoriska enhet som ansvarar för kontroll och rapportering av operativa risker som för övriga riskområden. En viktig fråga beträffande riskorganisation för alla riskområden är riskkontrollenhetens oberoende i förhållande till de enheter som ansvarar för att styra risktagandet. När det gäller operativa risker är detta speciellt besvärligt, emedan operativa risker finns i hela organisationen. I vissa företag ingår riskkontrollenheten i samma del av organisationen som kreditavdelningen, medan den i andra fall är direkt underställd vd eller någon annan befattningshavare som rapporterar direkt till vd. De mindre företagen har ofta en organisation där riskkontrollchefen rapporterar direkt till vd, medan det är vanligare att riskkontrollen organiseras tillsammans med kreditavdelningen på ett eller annat sätt i större banker.

När det gäller operativa risker har också internrevisions- och compliancefunktionerna en viktig roll. Internrevisionen har en viktig roll när det gäller att utvärdera den interna kontrollen och compliancefunktionen är givetvis väsentlig när det gäller risker som har med regelefterlevnad att göra. Även om dessa tre enheter i regel är (och bör vara) fristående från varandra har de flesta företagen sett till att rapporteringsvägar finns från exempelvis compliance till riskkontrollenheten för att säkerställa att den sammantagna rapportering över operativa risker som går upp till styrelsen är komplett. Detsamma gäller risker som identifieras inom säkerhetsområdet i de fall säkerhetsorganisationen inte är en del av riskkontrollfunktionen.

Eftersom operativa risker med nödvändighet måste identifieras och bedömas av personer som har god kunskap om de berörda processerna är det vanligt att riskkontrollenheten har kontaktpersoner för operativa risker i organisationens olika delar. Dessa ansvarar för att driva riskanalysprocessen och för att rapportera identifierade risker till den centrala riskkontrollenheten. Den centrala riskkontrollen gör normalt en aggregering av de olika enheternas riskanalyser och producerar därigenom en sammantagen bedömning av riskexponeringen för hela företaget som rapporteras till styrelse och vd.

Riskrapportering

Företagen skiljer sig mycket från varandra beträffande rapportering till styrelsen om operativa risker. Många företag har också under prövningens gång fått kritik av FI i detta avseende. I vissa företag har rapportering i princip saknats. Även bland de företag som har en mer omfattande rapportering är skillnaderna stora ifråga om innehåll och kvalitet.

De företag som håller högst kvalitet i rapportering har en relativt omfattande rapportering per halvår som innehåller en sammanställning av de riskanalyser som har gjorts för att ge en aktuell bild av företagets exponering mot operativa risker per affärsområde och riskkategori. Därtill rapporteras incident- och förluststatistik samt större enskilda incidenter och förluster.

Finansinspektionens rekommendationer

Ansvaret för central analys och kontroll av operativa risker bör ligga hos en riskkontrollenhet som är direkt underställd vd. Då riskanalysen under alla omständigheter kommer att vara baserad på kvalitativa bedömningar gjorda av personer som arbetar i de berörda processerna (genom exempelvis självutvärderingar) är riskkontrollenhetens oberoende viktigt för att säkra dualitet i riskbedömningen. Eftersom operativa risker finns överallt i organisationen, även i funktioner som inte har ett affärsansvar, är det bäst om den enhet som ansvarar för kontroll av operativa risker är direkt underställd vd.

Företagets styrelse och ledning bör få rapportering om operativa risker som åtminstone omfattar:

- sammanlagd exponering mot operativa risker baserad på företagets riskanalysmetod, omfattande samtliga kategorier av operativa risker
- information som möjliggör för mottagaren att se huruvida exponeringen ligger inom den toleransnivå som har fastställts
- statistik över incidenter och operativa förluster
- särskild information om större förluster eller incidenter
- riskbegränsande åtgärder som har vidtagits
- uppföljning av tidigare beslutade åtgärder.

Rapporteringen bör vara utformad på ett sådant sätt att mottagaren kan läsa och förstå rapporten utan en muntlig genomgång, även om en muntlig genomgång på styrelsemöte givetvis alltid bör ske. Alla operativa risker, inklusive säkerhetsrelaterade risker och compliancerisker, bör samlas i en rapport för att styrelsen och ledningen ska få en samlad bild av företagets riskexponering.

Fortsatt utveckling

Genom att uppfylla hanteringskraven i schablonmetoden kan företagen lägga grunden och gå vidare och utveckla mer avancerade metoder för att kvantifiera operativa risker. En strukturerad spårning och lagring av incident- och förlustdata är den viktigaste förutsättningen för att kunna utveckla de modeller och metoder som krävs för att uppfylla kapitaltäckningsreglernas krav. Det gäller den mest avancerade metoden för kapitaltäckning av operativa risker, nämligen internmätningsmetoden. FI ser gärna att företagen tar detta steg för att öka sofistikeringsgraden i sin riskhantering och få en starkare koppling mellan risk och kapitalkrav. Schablonmetoden är inte riskkänslig i någon större utsträckning.

Även med en mer avancerad metod för riskkvantifiering kan man emellertid aldrig bortse från att operativa risker i första hand är en processfråga. God internkontroll, kompetent personal samt hög kvalitet i processer och systemlösningar är de viktigaste faktorerna i hanteringen. Dessutom kommer avancerade statistiska modeller för kvantifiering av operativa risker också alltid att vara behäftade med stora modellrisker, varför de bör användas parallellt med subjektiva modeller som självutvärderingar eller processanalyser.